



# Balancing The Scales

Bill Boni

There is a rising tide of concern expressed by many commentators, concerning the advent of ever-broader workplace surveillance. In many places, especially the UK, video surveillance cameras have succeeded in reducing crimes against people and property, or at least in driving the crimes into the less desirable parts of the cities. There is now increased deployment of various products and technologies that allow employers to monitor not only employee's access and use of the Internet, but also to track and examine the contents of electronic mail messages. Indeed the recent example of hapless white collar employees sacked for misuse of their company E-mail to send risque or outright pornographic contents to friends and colleagues provides an example of the current state of electronic surveillance. In another case, Microsoft was tipped off about internal intruders only because they were monitoring outbound E-mail messages for their network and detected the presence of passwords in a message directed to an address in St. Petersburg, Russia.

Although most managers assume they have an unlimited right to monitor and manage employee use of E-mail and other networked capabilities, the counter position is gaining credibility and clout. After all, the new European Union data protection regulations address the importance of protecting 'sensitive' information against exploitation by third parties, and may actually circumscribe some of management's prerogatives regarding surveillance.

Meanwhile, across the Atlantic in the USA, legislation was introduced in 2000 that required employers to notify employees of the existence of monitoring and logging systems, and also to describe the purposes served by such monitoring.

There is every chance that the USA will finally establish, in the near future, some standards that will spell out what and how electronic workplace surveillance may be implemented.

On the one hand its possible we're seeing the evolution of the 'electronic sweat shop', where steely eyed Simon Legree managers use online monitoring as a tool to compel compliance with corporate edicts and to drive the workforce to higher levels of productivity.

On the other hand, as ever more of the value of the business is generated, stored and transmitted through E-commerce technologies, the potential for loss of digital forms of intellectual properties, and other digital assets, has also been increased, resulting in new risks that managers are responsible for managing.

There are also new risks arising out of the legal and regulatory environment in advanced industrial nations, that justify management attention.

The employee, who abuses their E-mail or Internet access privileges to send threatening, harassing or inflammatory, racist or derogatory messages, may trigger litigation that could result in substantial losses to his employer.

A wide range of tools have been created such as *Desktop Detective* from Omniquad ([www.omniquad.com](http://www.omniquad.com)) that allow even untrained staff or managers to turn up indications of employee abuse such as pornography. An additional product from this vendor offers the capability to filter outbound messages to ensure they do not contain unauthorized, offensive or proprietary contents.

Other sophisticated forensic technologies such as those offered by Vogon International ([\[tional.com/\]\(http://tional.com/\)\) or Guidance Software \(\[www.guidancesoftware.com/\]\(http://www.guidancesoftware.com/\)\), allow corporate security organizations to utilize the same technology developed for law enforcement to investigate abuses of computer systems. When wielded by professional and well-trained staff, under strict protocols, these are very powerful capabilities and certainly can even the odds on behalf of a company.](http://www.vogon-interna-</a></p></div><div data-bbox=)

What should be done to balance these competing, but not necessarily conflicting priorities? Well, even if there were no privacy and data protection laws or regulations, it seems that common courtesy demands that employees, consultants and contractors understand when and if they are subject to monitoring and logging, and the consequences that will prevail if a policy violation is detected.

Although some information security practitioners may groan of the thought of training the audience in these matters, this really is a great opportunity to reinforce the model behaviours that are consistent with business success in E-commerce.

Effective uses of Internet communications technologies are essential to E-commerce capability. Telling employees and other staff that their use of such tools will be monitored, will likely decrease the incidence and frequency of abuse. Most people understand that if they are caught violating company policies, they may well lose their jobs, so education should reduce the overall rate of abuse. To the extent that attracting and retaining technical talent are vital to success in E-commerce, playing fair with employees will support retention.

Outlining the company's policy and then monitoring to assure compliance with the policy, are steps that will establish and reinforce compliance with those policies. There is a great chance that much, if not all, serious violation will be deterred. Thus, key staff who might have violated policies will not do so, and will remain on the payroll to help the company prevail in its marketplace, rather than

moving on to accept work with the company's competitors.

The converse of all this is also likely to be true. To the extent that security groups perceive that their mandate is to entrap unwary violators and end their employment, the chance is great that management will find other, less expensive means of protecting their key assets, especially people.

It's also likely that lacking awareness of the company's rules and monitoring programmes, some greater percentage of the staff will take steps that violate relevant standards and may thus lose their jobs. Although terminations may be necessary on some occasions, it is a very unsatisfactory result, but an outcome that is predictable if the protection programme is purely reactive.

The challenge is to balance the risks to company assets, with a programme of education/awareness, monitoring and

swift but fair sanctions for violations of reasonable policies. If such a combination can be crafted, and implemented in a way that is consistent with pertinent legal and regulatory mandates, then the organization will have made a major contribution towards the creation of a more secure infrastructure that will support productive E-commerce applications.

The information security organization working on an E-commerce project must recognize that there are limits to what can be accomplished, and consult with experienced lawyers when devising their deployment and operational strategies. Although surveillance tools may seem to be an ideal weapon for combatting some aspects of the 'dark side' of E-commerce, they must be wielded with at least as much judgment as technical skill. Failure to do so may help create a bleak and oppressive darkness inside the very organizations they have been deployed to protect.

## Events Calendar

### FINANCIAL CRYPTOGRAPHY '01

19-22 February 2001. Location: Grand Cayman, BWI. Contact: website: <http://fc01.ai>

### THE WINTER 2001 BIOMETRICS SUMMIT

26-28 February 2001. Location: Miami, FL, USA. Contact: website: [www.biometricgroup.com/](http://www.biometricgroup.com/)

### EICAR 2001

3-6 March 2001, Location: Munich, Germany. Contact: website: <http://conference.eicar.org>

### COMPUTERS FREEDOM & PRIVACY 2001

6-9 March 2001. Location: Cambridge, Massachusetts, USA. Contact: E-mail: [infocfp2001.org](mailto:infocfp2001.org); website: [www.cfp2001.org/home.html](http://www.cfp2001.org/home.html)

### EUROSEC 2001

13-15 March 2001. Location: Paris, France. Contact: Isabelle Hachin, XP Conseil, 5 rue Aristide Briand, 92300 Levallois Perret, France; tel: +33 01 41 05 29 00; fax: +33 01 41 05 29 05; E-mail: [ihachin@xpconseil.com](mailto:ihachin@xpconseil.com); website: [www.xpconseil.com](http://www.xpconseil.com)

## PRIORITY ORDER FORM SPEED FAX: +44 (0)1865 843971

### PLEASE ENTER MY ORDER FOR

..... copies of Network Security ISSN 1353-4858  
12 issues US\$691/ NLG1360/ €617.14 [PCS65+B1]

EC Resident Customers (not UK) please add VAT at your national rate or state your VAT registration number.....

Plus VAT @ .....% US\$..... NLG..... €.....

**TOTAL PAYABLE US\$..... NLG..... €.....**

**IMPORTANT: Price is inclusive of postage and handling for all orders paid by credit card or cheque.** Invoices for orders without pre-payment will additionally be charged for postage and handling costs. Please note: Prices are subject to change without prior notice.

### PAYMENT (postage free of charge for orders with pre-payment)

Payment enclosed (please make cheques/Eurocheques payable to Elsevier)

POSTAGE FREE OF CHARGE

Please charge my Access/MasterCard/Visa/  
American Express/Barclaycard/Eurocard

(delete as applicable) POSTAGE FREE OF CHARGE

Card Number

Cardholder Name

Expiry Date

Today's Date

Signature

If you do not wish to receive promotional mailings from other companies please tick this box

If you do not wish to receive product related information from Elsevier Advanced Technology please tick this box

### DELIVERY ADDRESS

(please print clearly)

Name

Position

Approving Manager

Organisation

Address

Town

State

Post/Zip Code

Country

Tel number

Fax Number

E-mail

Nature of Business

### 4 EASY WAYS TO ORDER:

- 1) FAX PRIORITY ORDERS DEPARTMENT: +44 (0) 1865 843971**
- 2) E-MAIL YOUR ORDER TO [eatsales@elsevier.co.uk](mailto:eatsales@elsevier.co.uk)**
- 3) TELEPHONE PRIORITY ORDERS DEPARTMENT: +44 (0) 1865 843821**
- 4) POST YOUR ORDER TO: Priority Orders Department, Elsevier Advanced Technology, PO Box 150, Kidlington, Oxford OX5 1AS, UK**

### For US ORDERS

Elsevier Science, Regional Sales Office, Customer Support Department,  
655 Ave of the Americas, New York, NY 10010, USA

Tel: +1 (212) 633 3730

Fax +1 (212) 633 3680

Toll free: 1-888-437-4636 or 1-888-4ES-INFO

e-mail: [usinfo-f@elsevier.com](mailto:usinfo-f@elsevier.com)

When ordering please quote your customer KEYCODE - K10N9